[COMMITTEE PRINT]

98th CONGRESS *1st Session*	SENATE	REPORT No. 98-

FEDERAL COMPUTER SECURITY: AN ANALYSIS OF CONGRESSIONAL INITIATIVES AND EXECUTIVE BRANCH RESPONSIBILITIES

PREPARED FOR THE

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

OF THE

COMMITTEE ON GOVERNMENTAL AFFAIRS UNITED STATES SENATE

BY THE

CONGRESSIONAL RESEARCH SERVICE LIBRARY OF CONGRESS

1983.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE

24-870 O WASHINGTON : 1983

S402-16

COMMITTEE ON GOVERNMENTAL AFFAIRS

WILLIAM V. ROTH, JR., Delaware, *Chairman*

CHARLES H. PERCY, Illinois
TED STEVENS, Alaska
CHARLES McC. MATHIAS, JR., Maryland
WILLIAM S. COHEN, Maine
DAVID DURENBERGER, Minnesota
WARREN B. RUDMAN, New Hampshire
JOHN C. DANFORTH, Missouri
THAD COCHRAN, Mississippi
WILLIAM L. ARMSTRONG, Colorado

THOMAS F. EAGLETON, Missouri
HENRY M. JACKSON, Washington
LAWTON CHILES, Florida
SAM NUNN, Georgia
JOHN GLENN, Ohio
JIM SASSER, Tennessee
CARL LEVIN, Michigan
JEFF BINGAMAN, New Mexico

JOAN M. MCENTEE, *Staff Director and Chief Counsel*

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

WILLIAM V. ROTH, JR., Delaware, *Chairman*
WARREN B. RUDMAN, New Hampshire, *Vice Chairman*

CHARLES H. PERCY, Illinois
CHARLES McC. MATHIAS, JR., Maryland
WILLIAM S. COHEN, Maine
THAD COCHRAN, Mississippi
WILLIAM L. ARMSTRONG, Colorado

SAM NUNN, Georgia
HENRY M. JACKSON, Washington
LAWTON CHILES, Florida
JOHN GLENN, Ohio
JIM SASSER, Tennessee
JEFF BINGAMAN, New Mexico

S. CASS WEILAND, *Chief Counsel*
ELEANORE J. HILL, *Chief Counsel to the Minority*
KATHERINE BIDDEN, *Chief Clerk*

Congressional Research Service
The Library of Congress

Washington, D.C. 20540

FEDERAL COMPUTER SECURITY:

AN ANALYSIS OF CONGRESSIONAL INITIATIVES AND EXECUTIVE BRANCH RESPONSIBILITIES

Prepared at the request of the
Senate Committee on Governmental Affairs
Permanent Subcommittee on Investigations

Louise G. Becker
Specialist in Information Science and Technology
Science Policy Research Division

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
Washington, D.C.

PREFACE

During the 97th Congress, the Senate Permanent Subcommittee on Investigations became concerned about the susceptibility of modern computer systems to fraud and other criminal abuses. The Subcommittee initially directed its examination to the question of whether federal and commercial computer systems are adequately protected from criminal abuse, and if new legislative or regulatory protections are required.

In 1976 and 1977 the Committee on Governmental Affairs issued a study and a staff report on the security of federal computer systems which concluded that additional steps must be taken to ensure that federal computer systems are secure from illegal intrusions. It is the intention of this Subcommittee to examine federal computer systems to assess what protections were developed as a result of earlier efforts, how effective those protections have been, and whether further protections should be implemented due to technological advances in the computer industry.

It is also this Subcommittee's intention to examine existing federal statutes in order to determine whether they are fully applicable to the criminal schemes affecting modern computer operations.

The Library of Congress was asked to review federal concerns and policy options concerning computer and information systems security. The Subcommittee is grateful to Louise G. Becker of the Congressional Research Service for her detailed examination of this topic, and for her assistance to the Subcommittee staff.

WILLIAM V. ROTH, JR.,
Chairman,
Permanent Subcommittee on Investigations.

CONTENTS

	Page
I. INTRODUCTION	1
A. Nature and Scope of the Problem	1
B. Abuses and Safeguards	2
C. Major Issues	3
1. Resource Allocation and Ordering Priorities	3
2. Other Issues	3
II. CONGRESSIONAL INITIATIVES	5
A. Congressional Interest and Concerns	5
1. Some Problems Encountered in Safeguarding Federal Systems	5
2. Fraud and Abuse	7
B. Computer Crime Legislation and Hearings	8
C. Related Computer Security Interests	11
1. Federal Computer Security Management Problems	11
2. Computer Security and Information Exchanges	12
a. Privacy and Confidentiality	13
b. Implications of Technology Transfer	14
c. Government Secrecy and Classification	14
III. EXECUTIVE BRANCH RESPONSIBILITIES AND ACTIONS	17
A. Executive Branch Problems Cited in GAO and Congressional Reports	17
1. Failure to Implement Computer Security Programs	18
2. Limited Support by Senior Management	18
3. Problems in Implementation of TM-1	19
4. Difficulties in Instituting Controls	20
B. Central Management Agencies	20
1. Office of Management and Budget	20
a. Lack of Strong Leadership	21
b. OMB's Organization	21
2. General Services Administration	21
3. Other Central Management Agencies	22
C. Department of Defense	22
IV. APPENDIX	25

I. INTRODUCTION

Information technologies, including computers, telecommunications networks, and word processors, provide operational support for a modern Government. While these technologies are valuable resources in themselves, the data and information handled by these innovations often also represent a considerable investment. The Federal Government, one of the largest users of computers, reported that in 1980 it had over 15,000 computers in its inventory.[1] A report by the General Accounting Office [GAO] in the late 1970's indicated that the estimated cost of operation of Federal systems was well over $10 billion.[2]

Computer-communication security, in the context of this report, is viewed as the protection of a broad spectrum of activities related to the life-cycle management of computerized resources. It specifically relates to those functions which assure that information is maintained with adequate confidentiality, accuracy, integrity, and availability to meet Federal goals and objectives. Government dependence on an investment in information resources necessitates appropriate safeguards to protect these assets against actual and possible threats. In addition, it gives impetus to a continuing review of Federal policies and activities designed to protect these resources. This report provides an analysis of selected congressional initiatives and Federal responsibilities related to computer security. Many of the observations included here are based on a more comprehensive Congressional Research Service report entitled, "Computer Security: An Overview of National Concerns and Challenges."[3]

A. Nature and Scope of the Problem

Computers and associated technologies are used in supporting programs ranging from national defense, intelligence, and space to air traffic control, health, social welfare, and financial activities. Traditionally, computer security was examined within the context of individual areas, such as national defense, personal privacy, Federal information resources management, and computer crime. For example, in the past the stringent computer-communication security requirements of the national defense community were not considered applicable to the civilian sector. More recently, an in-

[1] U.S. General Services Administration. "Automated Data and Telecommunications Service." "Automatic Data Processing Equipment Inventory in the United States." Washington, D.C., U.S. Government Printing Office, 1981. p. 29.

[2] U.S. Comptroller General. "Automated Systems Security—Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data" LCD-78-123, Jan. 23, 1979. Washington, D.C., U.S. General Accounting Office, 1979. p. 8. Hereafter referred to as GAO. Automated Systems Security." " "

[3] U.S. Library of Congress. Congressional Research Service. "Computer Security: An Overview of National Concerns and Challenges." Report No. 83-135 SPR [Multilith] Feb. 3, 1983. Authored by Louise G. Becker. Washington, D.C., 1983. 241 p.

24-810 O - 83 - 2

creased appreciation of the value inherent in certain civilian systems (for example, financial data) has prompted attention to improving their security as well. Furthermore, it is increasingly recognized that because these topics often share similar problems and may be amenable to similar solutions an integrated approach to computer security may be warranted.

In certain environments computer security is an integral part of an agency's mission and therefore receives a high priority. For example, the national security community's strong commitment to computer security is evidenced by personnel clearance, support of research and development of computer security tools and techniques, and an integrated security program. While not all elements of the national defense community's security approach are appropriate to all Federal agencies, the growing importance and value of civilian agency systems may require a similar effort. At the same time, however, appreciation of differences in agency requirements as well as differences in applications and systems needs is critical to assessing the Federal Government's direction and approach to computer security.

An awareness of the threats to computer systems and the value of computerized resources influence the desire to safeguard automated information resources in cases where computer security requirements are not an outgrowth of the agency mission. A lack of understanding of the problem coupled with a reluctance to commit resources for the computer security effort are major barriers to instituting good security practices. Many agencies find it difficult to pinpoint responsibilities or place controls to protect computerized resources. In some cases agencies may not be motivated to institute computer protections until there is an incident or specific damage. Furthermore, the reporting or discovery of an abuse does not guarantee that a remedial action will take place. Managers may be reluctant to take action to correct a situation. Some may believe that the incident will not be repeated. Others may fear that the system or institution will be mistrusted if the incident is publicly known.

B. Abuses and Safeguards

Computer vulnerabilities and abuses are associated with both technical and nontechnical factors. Compromise and damage to data and computer systems vary from simple to sophisticated threats.[4] The vulnerabilities inherent in a system may be associated with the data, equipment (hardware), computer instructions or programs (software), and communication networks. Some major threats to computerized resources are the result of:

—Undesired personnel actions (intentional and unintentional);
—Theft of data, services, or equipment;
—Internal systems weaknesses;
—Network problems;
—Failure of support services (air-conditioning, electric power, transportation); and
—Lack of access controls (passwords, et cetera).

[4] Including those from personnel actions; natural hazards (for example, fire, water, earthquakes); criminal activities; technical weaknesses; electrical power fluctuations; nuclear threats and emanations (for example, electronic magnetic pulses [EMP]).

Computer security safegards [5] include a broad range of techniques and tools designed to protect data and equipment as well as related communications networks. Techniques and tools associated with computer security include: identification of individuals who may have access to data or services; monitoring of computer operations (checking transactions and processes); and maintenance of systems integrity (assuring performance, reliability, and availability of the systems).

C. Major Issues

1. RESOURCE ALLOCATION AND ORDERING PRIORITIES

The allocation of resources is central to an effective Federal computer security program. Therefore, Federal agencies must weigh the possible loss of data and availability of services against the investment in costly computer security measures. Maintaining a balance between systems integrity or reliability and instituting controls is critical.

Agency goals and objectives may not be sufficiently defined to give a basis for assigning priorities relating to computer security. A narrow interpretation of mission goals may result in ignoring sound computer security practices. For example, an agency may place a higher priority on meeting a specific mission requirement (such as sending out welfare or social security checks) than on maintaining sound computer security procedures. The result is that in a crisis the mission requirement is pursued and the security measure dismissed. This condition is referred to as "mission override."

2. OTHER ISSUES

Other Federal computer security issues include questions regarding:

—The adequacy of national security and defense communities computer security efforts and the technical approach of DOD computer security initiatives;
—The adequacy of Federal computer resource protection and policies;
—The implications of computer-related crime problems, especially as they relate to Federal computer systems;
—The commitment to privacy and confidentiality in personal record systems;
—The implications of new technologies and applications, such as electronic message systems, electronic funds transfers [EFT], robotics and automated manufacturing systems;
—The debate concerning encryption systems, including the adequacy of the Federal Data Encryption Standard [DES]; and
—The problems of secrecy, private sector inventions, and technology transfer.

---

[5] These safeguards may be categorized or classified as physical, technical, or administrative measures. These safeguards may be directed at protecting the computer security facility, equipment, software, materials (computer tapes, related documentation, forms, logs), data networks and communication links, data within the system, and information products.

II. CONGRESSIONAL INITIATIVES

Congress is increasingly interested in computer security, especially as it relates to national programs and Federal systems. In particular, Congress is concerned with protecting national security information resources, the effectiveness of Government computer systems,[6] privacy and confidentiality of certain records systems, and the protection of Government systems from fraud and abuse.

A. Congressional Interest and Concerns

1. SOME PROBLEMS ENCOUNTERED IN SAFEGUARDING FEDERAL SYSTEMS

The General Accounting Office [GAO], in response to congressional concerns, has investigated a variety of Federal agency computer security efforts. Specifically, the GAO has reported on issues related to privacy concerns, computer abuse and criminal activities, vulnerability of Government communication systems, contingency planning, and the effective management of Government agency computer systems.

Some of the GAO investigations have focused on specific Federal Government computer security operations, such as those in the Internal Revenue Service, the Social Security Administration, and the Community Services Administration.[7] Other GAO investigations have called attention to Government-wide policies and directives. The major findings of these latter studies are discussed in this section and in section III of this report.

The General Accounting Office's review of Federal automated information systems security management indicates that there is a lack of coordination in assisting agencies to develop effective computer security management programs.[8] The GAO is critical of the limited support Federal agencies give to computer security efforts and the lack of leadership provided by the responsible central management agencies.[9] GAO claims that the failure of the central management agencies to encourage computer security efforts

---

[6] For additional information on Federal computer management see: U.S. Library of Congress. Congressional Research Service. Federal Information Management Policy: Critical Directions. Report No. 81-101 SPR [Multilith], June 1980 Updated March 1981. Authored by Louise Giovane Becker. Washington, 1981. 187 p.

[7] Reports of the General Accounting Office that may be of interest include: "IRS' Security Program Requires Improvements to Protect Confidentiality of Income Tax Information." (GGD-77-44, July 11, 1977); "Flaws on Controls Over the Supplemental Security Income Computerized System Causes Millions in Erroneous Payments." (HRD-79-104, Aug. 9, 1979); and "Solving Social Security's Computer Problems: Comprehensive Corrective Action Plan and Better Management Needed." (HRD-82-73, Aug. 23, 1980).

[8] U.S. General Accounting Office. "Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices." MASAD-82-18, Apr. 21, 1982. Washington, D.C. 1982. Hereafter referred to as GAO. "Federal Information Systems Remain Highly Vulnerable * * *."

[9] The central management agencies related to computers and associated activities include: Office of Management and Budget; the General Services Administration; the Department of Commerce (National Bureau of Standards), and the Office of Personnel Management.

throughout the Government harms Federal productivity. Specifically, they state that the lack of guidance to improve the safeguarding of automated information systems by Federal agencies limits computer security initiatives.[10] In this regard, the GAO expressed concerns that the Office of Management and Budget [OMB], Circular A-71, Transmittal Memorandum No. 1, "Security of Federal Automated Information Systems." [TM-1] does not: [11]

—Identify the minimum controls necessary for ensuring a reasonable level of protection over personal, proprietary, and other sensitive information;

—Clarify the relationship between Transmittal Memorandum No. 1 and policy and guidance on safeguarding information classified for purposes of national security;

—Clarify when executive agencies must afford the same level of protection against unauthorized disclosure of personal, proprietary and other sensitive information as they do to information classified for purposes of national security; and

—Establish policy and specific guidance for achieving a reasonable level of protection over those systems using telecommunications networks.

In addition, the GAO indicated that the executive agencies have not taken action to assure a "reasonable level of protection" of automated information resources.[12]

The growth in the number of Federal agencies using computer networks greatly increases the potential for abuse in unprotected systems. GAO lists some 31 major Federal dedicated networks having wide geographic distribution. This dependency on networks and the increases in data and resource sharing presents a danger to certain systems. The considerable investment in automated systems development and possible expansion of services contributes to the concern that these systems may be vulnerable.[13] Consequently, GAO has stressed the need to secure these resources by expanding Federal policies, such as TM-1, to include network security.[14]

The GAO also has criticized the lack of OMB leadership. This is believed to contribute to a lack of support by Federal senior managers in allocating resources to protect computerized resources. Another criticism voiced by GAO is that the broad social goals of privacy (that is, Privacy Act of 1974) and fair information practices (Freedom of Information Act) have not been translated into precise steps for use in designing, implementing, operating, and maintaining computer systems security. Therefore the central management agencies have been urged by GAO to improve guidance to Federal agencies in these areas.[15]

In summary, there are difficulties in determining the level of security that sensitive information requires, according to GAO. Limited Federal-wide guidance, lack of security direction for telecommunication networks, and the issuing of uncoordinated policies,

---

[10] GAO. "Federal Information Systems Remain Highly Vulnerable * * *." Op. cit.
[11] Ibid., p. 9.
[12] Ibid., p. i.
[13] Ibid., p. 5-7.
[14] U.S. General Accounting Office. "Increasing Use of Data Telecommunications Calls for Stronger Protection and Improved Economies." Nov. 12, 1980. LCD-81-1. Washington, D.C., 1980. 69 p.
[15] GAO. "Federal Information Systems Remain Highly Vulnerable * * *" Op. cit., p. 3.

standards, and guidelines contribute to the present set of problems facing the Federal manager.[16] Lack of the leadership by OMB required by the Paperwork Reduction Act of 1980 further reduces the impact of a computer security program. As a result, GAO reports, Federal managers have not allocated resources nor have they established priorities for instituting computer security measures.

Another problem which GAO indicated contributes to the less than adequate Federal security effort is the lack of contingency planning. A lack of understanding of the importance of backup has resulted in poor disaster management.[17] Computerized resources are sensitive to electrical power fluctuations. These fluctuations and outages cause loss of data and services. In reviewing Federal agencies' emergency plans, GAO discovered that agency planning for recovery from massive electrical power failure is inadequate.[18]

2. FRAUD AND ABUSE

Fraud and abuse in Federal automated information systems continues to be a central concern.[19] The GAO and congressional reports indicate a wide range of problems, including the lack of Federal controls over many sensitive systems. Government computers, GAO reports, process: [20]

—Unreviewed authorizations for payments or checks (excluding payroll) totaling $26 billion;
—Unreviewed bills totaling $10 million; and
—Unreviewed requisitions, shipping orders, repair schedules, and disposal orders for materials valued at $8 million.

In addition, "undetected data and program errors cost the Government many million dollars annually and can impede agency mission achievement".[21]

The staff investigations by the Senate Committee on Government Operations (now the Committee on Governmental Affairs) in the late 1970's indicated the widespread problems of computer fraud and abuse. The 1976 GAO investigations [22] in support of the committee's efforts further documented Federal agency problems in securing computerized resources. Specifically, Federal agencies had difficulties in instituting auditing safeguard measures for inventory control, as well as putting in place physical security measures. In addition, the committee found that Federal computer systems were

---

[16] Ibid.

[17] U.S. General Accounting Office. "Most Federal Agencies Have Done Little PLanning for ADP Disasters." Dec. 18, 1980. AFMD-81-16. Washington, D.C., 1980. 20 p.

[18] U.S. General Accounting Office. "Federal Electrical Preparedness is Inadequate." May 12, 1981. EMD-81-50. Washington, D.C., 1981. 40 p.

[19] A recent document issued by Department of Health and Human Services' Inspector General, "Computer-related Fraud and Abuse in Government Agencies," Washington, D.C., June 1983, outlines the scope of the problem in Federal systems. In addition, a new system, fraud and corruption tracking [FACT], operated by the Department of Justice, is designed to indicate when a case involves a computer.

[20] U.S. General Accounting Office. "GAO Findings on Federal Internal Audits—A Summary." May 27, 1980, FGMSD-80-39. Washington, D.C. 1980. p. 17.

[21] Ibid.

[22] The GAO reports: "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout Federal Government," April 23, 1976, B-115369; "Computer Crimes in Federal Programs," Apr. 17, 1976, B-115369: "Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities," May 10, 1976, B-115396.

vulnerable to a wide range of abuses, including computer crime.[23] A subsequent report of the committee found that not only was there a need to improve the physical security in Federal computer systems, but that the lack of personnel security was detrimental to Federal systems.[24] As a result, the committee recommended that personnel security be improved and that this improvement be accelerated for those having access to "classified and national security information; * * * those concerned with the distribution of public funds; and * * * those offering the opportunity to divert or otherwise abuse highly valuable private or economically valuable data." [25] The committee further recommended that administrative and legislative measures be developed. In response to these recommendations OMB issued a set of computer security guidelines on personnel security. Subsequently, Senator Abraham Ribicoff, then chairman of the Senate Committee on Government Operations, introduced in the 95th Congress the first legislative measure to protect Federal computer systems, as described below.

B. Computer Crime Legislation and Hearings

Senator Ribicoff's bill, S. 1766, the Federal Computer Systems Protection Act of 1977, was designed to protect computers in use in the Federal Government as well as those that use a facility of interstate commerce. The bill was designed to prevent four categories of computer crime, namely: [26]

—The introduction of fraudulent records or data into the computer system;
—The unauthorized use of computer-related facilities;
—The alteration or destruction of information or files; and
—The stealing, whether by electronic means or otherwise of money, financial instruments, property, services or valuable data.

Hearings on the bill were held by the Senate Committee on the Judiciary. Witnesses indicated general support for the intent of S. 1766, but offered reservations regarding the breadth of the bill. Specifically, some witnesses expressed concern that the bill might expand Federal jurisdiction to include many private sector computer systems because these systems use a communications carrier involved in interstate commerce. Another problem witnesses alluded to was that the term "computer" might be too broadly interpreted and could include any device from a pocket calculator to large multifaceted computer-communications systems.[27] The possible expansion of Federal jurisdiction and the lack of a concise definition were other major concerns. Another factor limiting support for the

---

[23] U.S. Congress. Senate. Committee on Government Operations. "Problems Associated with Computer Technology in Federal Programs and Private Industry: Computer Abuse." Committee print, 94th Congress 2d session, Washington, D.C.. U.S. Government Printing Office, 1976. 448 p.

[24] U.S. Congress. Senate. Committee on Government Operations. "Computer Security in Federal Programs." Commitee Print, 95th Congress 1st session, Washington, D.C., U.S. Government Printing Office, 1977. p. 267

[25] Ibid.

[26] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Criminal Laws and Procedures. Federal Computer Systems Protection Act. Hearings on S. 1766, held June 21 and 22, 1978, 95th Congress, 2d session, Washington, D.C., U.S. Government Printing Office, 1979, p. 1.

[27] Ibid., p. 35.

legislation was the possible effect it might have on new applications of technology, such as electronic funds transfers. Witnesses suggested that these special applications might require more specific statutory controls.[28] The problem of prosecuting computer frauds and the lack of trained criminal justice officials knowledgeable about computer crime actions also prompted negative reactions to the measure.

On the other hand, supporters of S. 1766 believed that in addition to protecting Federal computer systems, the bill would improve overall computer management. The legislation, these supporters contended, also would raise the level of awareness and could stimulate the development of training programs for criminal justice officials designed to improve their ability to identify and prosecute computer criminals. The basic disagreement regarding the legislation's scope and intent hampered final action on the measure. Many of the advantages and disadvantages of S. 1766, as discussed by witnesses at these first hearings, remain relevant to subsequent Federal computer crime bills.

In the 96th Congress, Senator Abraham Ribicoff introduced S. 240, the Federal Computer Systems Protection Act of 1979. The bill, although modified, paralleled the bill on computer crime previously introduced in the 95th Congress. A 1-day hearing [29] by the Senate Committee on the Judiciary, Subcommittee on Criminal Justice, was prompted by concerns that Federal criminal jurisdiction would be expanded by S. 240. At the hearing, Senator Hatch expressed concerns that this legislation was not needed since there were over "40 sections of the United States Code, provisions of the Electronic Funds Transfer Act, provisions of the Financial Institutions Act and provisions of the Privacy Act, that have direct utility to Federal prosecutions of computer abuse." [30]

Senator Laxalt echoed these reservations and expressed concern that S. 240 "not only adds new substantive offenses to the Criminal Code, it expanded Federal criminal jurisdiction in such a way that the wire and mail fraud statutes pale by comparison." [31] Furthermore, the legislation was believed to expand Federal criminal jurisdiction into areas not previously covered, especially those reserved to the States. Senator Laxalt also questioned the limited understanding of the scope and nature of computer crime, citing the lack of information on incidences and costs of computer crime. Also questioned was whether Congress "properly understood the intricacies and dimensions" of this complex problem.[32]

Witnesses at the hearings supported these same concerns and noted that the limited experience with State computer crime legislation had not provided any solid information on the success of such legislation in prosecuting computer criminals.[33] One witness was especially concerned that the bill be amended so that the only computer systems affected would be those owned or operated for

---

[28] Ibid.

[29] U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Criminal Justice. Computer Systems Protection Act of 1979. Hearings on S. 240, held Feb. 28, 1980, 96th Congress, 2d session, Washington, D.C., U.S. Government Printing Office, 1980, 179 p.

[30] Ibid., p. 1-2.

[31] Ibid., p. 3.

[32] Ibid.

[33] Ibid. p. 6.

the exclusive use and benefit of the U.S. Government.[34] Another argued that computer crime could adequately be dealt with by present laws.[35] The lack of evidence and information on the scope of the problem [36] coupled with the concern that the legislation would duplicate existing criminal codes limited further consideration of S. 240 by the 96th Congress.

In the 97th Congress, Representative Bill Nelson introduced H.R. 3970, the Federal Computer Systems Protection Act of 1981. H.R. 3970, similar to S. 240, received no floor action in the 97th Congress, but hearings by the House Committee on the Judiciary, Subcommittee on Civil and Constitutional Rights did examine the subject of computer crime. Witnesses from the Department of Justice discussed the phenomena of computer crime, but did not support the need for legislation.

Other witnesses cited the lack of accurate reporting on computer crimes and the difficulty in understanding the total dimensions of the computer crime as major barriers to establishing Federal laws in this area. There also was some disagreement between witnesses on the applicability of State statutes. The statement by one witness that State computer crime statutes had not been used was refuted by Representative Bill Nelson. The Congressman pointed out that the Florida statute was being used and a case was pending. Finally, some witnesses suggested that a Federal commission should be created to explore and investigate the nature and scope of computer related crime.

Although there have been objections to some aspects of the previously introduced computer crime legislation, Members of Congress continue to assess the implications of computer abuse and the lack of emphasis on computer security in certain Federal systems. Congressional investigations, findings of the General Accounting Office, and a recent report entitled, "Computer-Related Fraud and Abuse in Government Agencies," issued by the Inspector General, U.S. Department of Health and Human Services, indicate a range of computer abuses and problems associated with unprotected automated information systems. In addition, some prosecutors maintain that existing laws may be insufficient to support convictions in cases of computer abuse. Some believe that the special circumstances associated with computer abuse require direct and clear statutory language to convict and sentence the computer criminal.

In the 98th Congress four bills have been introduced that concern computer crime: S. 1733 and H.R. 1092, Federal Computer Systems Protection Act, introduced by Senator Paul S. Trible and Representative Bill Nelson, respectively. These measures are similar to legislation on computer crime considered by previous Congresses; H.R. 3075, the Small Business Computer Crime Prevention Act, introduced by Representative Ron Wyden; and H.R. 3570 a bill to protect against computer credit card fraud, introduced by Represention William J. Hughes. Hearings have been held on H.R. 3075

---

[34] Ibid. p. 9
[35] Ibid., p. 47.
[36] The newly established FACT systems in the Department of Justice is designed to correlate the incidence of computer crime.

and additional hearings are expected on the other measures during this Congress.

C. Related Computer Security Interests

Congressional concern with protecting Federal computers and information resources has not been limited to threats of computer crime. Over the years Congress has focused on other aspects of computer and communication security in Federal systems as well. Congress has been supportive of actions to strengthen Government management of computer and information systems, protect sensitive information, and limit disclosures and dissemination of certain information.

Present Federal computer security policies emerge from a broad range of statutory requirements and associated administrative directives. These policies, which seek to protect national security related information systems, preserve privacy, improve effectiveness of automated information systems, and safeguard Federal resources from abuse, have been supported by Congress.

Beginning in the mid-1960's Congress sought to improve Federal management of computers. The enactment of Public Law 96-306, generally referred to as the Brooks Act, provides a basic foundation for some Federal computer security management activities. Specifically, the Brooks Act focuses on Federal computer related activities in the central management agencies.[37] As a result of this focus, computer security activities have included the development of standards and guidelines. Federal information processing standards and related guidance on computer security will be discussed in detail in section IV of this report.

As part of the continuing interest and concern for effective management of Federal computer and information resources, Congress enacted the Paperwork Reduction Act of 1980 (Public Law 96-511). The act is designed to strengthen Federal information activities. A principal element of the act is the concept of information resources management [IRM] which provides a major framework for Federal managers.[38] The act's two-prong approach—to reduce the burden of paperwork in Federal Government and to improve Government management of information resources—represents a change in Federal computer management. The legislation and followup congressional oversight have given special emphasis to coordinating information resources and the need for periodic agency-wide reviews of computer and information technology activities.

1. Federal Computer Security Management Problems

Congress continues to examine, through its oversight and appropriation functions, the activities of certain Federal agencies in protecting computer and information systems resources.

In the 97th Congress, the House Committee on Government Operations found that a lack of controls contributes to mismanagement of certain Federal computer systems. According to the com-

---

[37] See footnote 9.

[38] Information resources management has been viewed as improving computer security management in that it provides for top level management direction and central coordination. The IRM concept may be viewed as an integral part of computer and information protection.

mittee, some agencies had not adequately protected their systems from computer abuse. The lack of awareness of the problem often was cited as limiting the planning and allocation of resources to cope with existing or potential abuses in Federal agencies. As an example of this problem the House Committee on Government Operations reported that the potential for massive fraud within the Social Security Administration [SSA] was critical.[39]

The committee noted that problems highlighted by the GAO in a series of reports in the late 1970's had not been remedied and that the GAO recommendations had not been followed. The committee reported that a recent investigation by the GAO [40] indicated that not only had SSA failed to implement the GAO recommendations, but additionally they had not put into action those suggestions made by internal and external audit agencies.[41] The committee further observed that Federal computer systems were often compromised by individuals who possessed limited knowledge of the system and had few operational skills. The committee expressed concern that an unprotected SSA computer system presents an excellent opportunity for those with criminal intent.[42] As a result, the committee recommended that the Department of Health and Human Services' Inspector General review all SSA security procedures and report to the Congress by early 1983.[43]

2. COMPUTER SECURITY AND INFORMATION EXCHANGES

Federal computer security has not only involved the overall management of Federal computer and information resources or the specific actions of Federal agencies, but has also been concerned with broader concepts and problems. Implicit in congressional activities related to privacy and confidentiality, technology transfer, and Government secrecy is the need for improved computer security.

In the late 1960's, Congress addressed the possible erosion of personal freedoms through the misuse of certain records and associated information technologies. The potential danger arising from abuses in computerized systems continues to draw attention to the need for security of sensitive systems. By the mid-1970's Congress enacted the Privacy Act of 1974 (Public Law 93-597) and amendments to the Omnibus Crime Control and Safe Street Act (Public Law 93-83) to improve protection of personal data. These statutes called for specific security measures to protect information regarding an individual and to limit unwarranted disclosures. By the late 1970's, reflecting the growing concern for the protection of Government resources, Congress enacted laws to establish offices of the Inspector General [IG] in some Federal agencies.[44] The purpose of

---

[39] U.S. Congress. House. Committee on Government Operations. "Mismanagement of SSA's Computer Systems Threatens Social Security Programs." House Report No. 97-900, 97th Congress 2d session, Washington, D.C., U.S. Government Printing Office, 1982. Hereafter referred to as House Report No. 97-900.

[40] See: U.S. General Accounting Office. "Solving Social Security's Computer Problems: Comprehensive Corrective Action Plan and Better Management Needed." HRD-82-19, Dec. 19, 1981.

[41] House Report No. 97-900, op. cit., p. 12.

[42] Ibid.

[43] Ibid., p. 17.

[44] For example in the 94th and 95th Congresses, legislation was enacted to establish an inspector general's office in the Department of Health, Education, and Welfare (now the Department of Health and Human Services), (Public Law 94-505); in 12 other Federal agencies (Public

Continued

these offices is to eliminate fraud, abuse, and waste from Government. Since many Federal Government operations are automated, these IG offices are viewed as a means to protect computer systems from abuse.

a. Privacy and confidentiality

Over the years, the Congress has recognized the significance of protecting certain Government information from unwarranted disclosures and has enacted specific legislation with provisions for confidentiality of data collected by agencies (for example, Census, Internal Revenue Service, and Social Security Administration). The desire to minimize Government intrusion into the lives of citizens and the need to protect personal freedoms has continued to stimulate congressional interest.

Congress has been concerned specifically with proposals for excessive data sharing of personal record systems within Federal agencies and the lack of strong Federal guidance to prevent abuses in data sharing among Federal agencies. The Privacy Act of 1974 (Public Law 93-597) is designed to safeguard individual privacy by protecting personal information held by Federal agencies. The Federal agencies are required by the act to establish rules to protect systems and to limit unwanted dissemination of these records. Congressional concerns over implementation of the act stem from the fact that (1) many agencies have given privacy related matters a low priority; (2) implementation, while conforming to the letter of the law, has not always reflected the spirit of the law; and (3) there is an increase in exchanges among Federal agencies of critical data. A GAO review of Federal agency compliance with fair information practices statutes indicated that privacy laws are successful when the public is informed regarding the law and rights of access to the records.[45]

Congress amended the Omnibus Crime Control and Safe Street Act through passage of the Crime Control Act of 1973 (Public Law 93-83), to provide that criminal history information be protected to ensure security and privacy. Section 524b of the statute limits the use of criminal history records and allows correction of data. Subsequently, Federal and State agencies which maintain criminal justice records have developed systems to meet resulting regulations.[46] However, the problems of implementing the laws and some operational limitations have generated some concern. A MITRE Corp. report, "Implementating the Federal Privacy and Security Regulations," commented that progress in implementation of security requirements was dependent on: prior involvement, a commitment to privacy and security, and a mandate regarding specificity of file content.[47] In the case of criminal justice systems, some fac-

---

Law 94-52); and the Department of Energy (Public Law 95-1). In 1981, an inspector general's office for Department of Defense was created by the Department of Defense Authorization Act of 1983 (Public Law 97-252).

[45] U.S. Comptroller General. "An Informed Public Assures that Federal Agencies will Better Comply with Freedom of Information/Privacy Laws." Oct. 24, 1979. LCD-80-8. Washington, D.C., U.S. General Accounting Office, 1979. 53 p.

[46] U.S. Department of Justice regulation: 40 Federal Register 22114 and as amended 41 Federal Register 11714.

[47] MITRE Corp. METREX Division. "Implementating the Federal Privacy and Security Regulations." Vol. I and II. MITRE Technical Report MTR 7704. McLean, Va., 1977.

tors impeding implementation of security include: lack of sufficient resources, confusion as to interpretation of the regulations, traditional practices inhibiting change, and difficulty in linking security requirements with proposed automated data systems.[48] These problems may be applicable to other computerized sensitive information systems.

b. Implications of technology transfer

Hearings and a report issued by the Senate Committee on Governmental Affairs, Permanent Subcommittee on Investigations in the 97th Congress indicated concern with the transfer of high technology to Soviet bloc nations.[49] Although computer security technologies are not specifically addressed in the subcommittee's report, it is clear that the dissemination of sensitive innovations may require additional oversight. Certain computer security technologies have implications for national security and therefore indiscriminate dissemination of transfers presents a problem.

It is assumed that sensitive computer security technology is especially targeted by the Nation's adversaries. The subcommittee's investigations indicated that there is an ongoing and active effort on the part of the Soviets to obtain high technology, including computer security technology, by reviewing all open literature, creating "Communist-owned firms in the United States and elsewhere," bribing persons with sensitive information, and exploiting scientific exchange programs.[50] Consequently the subcommittee's recommendations to control technology transfers merit special consideration with regard to sensitive computer security technologies.

In a followup report the subcommittee indicated that there was a lack of strong enforcement programs and limited intelligence on which technologies should be controlled. The subcommittee staff called for better enforcement, consideration of coordination and reorganization of enforcement operations, and improved information exchange to aid in identification of critical technology.[51]

Another problem noted by the subcommittee was that much of the equipment and techniques associated with computer security can be classified as "dual use" technology that may be used for civilian or military purposes. This further complicates the classification of computer security innovation in technology transfers.

c. Government secrecy and classification

The House Committee on Government Operations in the 96th Congress examined the problem of maintaining secrecy and Government control over the private sector. The committee reviewed executive branch support of secrecy in public cryptology research

---

[48] Becker, Louise Giovane. "Security and Privacy of Criminal Justice Information Systems: Innovation and Political Reality." In proceedings of the 1980 International Carhahan Conference on Security Technology. Berlin, West Germany. October 1980. Lexington, Ky., University of Kentucky. p. 8.

[49] U.S. Congress. Senate. Committee on Governmental Affairs. Permanent Subcommittee on Investigations. "Transfer of United States High Technology to the Soviet Union and Soviet Bloc Nations." Hearings, May 4, 5, 6, 11, and 12, 1982. 655 p.

[50] Ibid., p. 5

[51] U.S. Congress. Senate Committee on Governmental Affairs. Permanent Subcommittee on Investigations. "Transfer of United States High Technology to the Soviet Union and Soviet Bloc Nations." Senate Report No. 97-664. Washington, D.C., U.S. Government Printing Office, 1982. 69 p.

and the handling of sensitive inventions developed by the private sector. The House committee assessed the voluntary program of Government review for cryptology research papers or articles prior to publication and concluded that it would have a chilling affect on research. The committee questioned the National Security Agency [NSA] review process and the implications of such a program. They expressed concern regarding restricting the dissemination of certain technologies or methodologies in an effort to prevent access to critical information or equipment by the Nation's adversaries. The committee further questioned the potential effect on free enterprise and the implications for the private sector. The investigation suggested that there is a need to improve Government control over sensitive information. They also suggested streamlining the process, strengthening administrative controls and improving the approach presently used in instituting controls.[52]

Another set of concerns identified by the committee arises from private sector rights to market and use inventions and ideas. The committee stated that the need to restrict sensitive tools and techniques which may compromise national security should be balanced against the adverse impact on the free flow of information. The full consequences of limiting or restricting information are not always known. Fundamental questions surround the appropriate role of Government and the advisability of instituting certain controls. The need to protect the Nation while remaining supportive of private initiatives remains a critical problem.

In the 97th Congress the House Committee on Government Operations examined Executive Order 12356, Security Classification Policy.[53] Of special interest to the computer security arena is that the Executive order and its predecessors provide the policy framework for most automated systems handling classified data. The committee specifically expressed concern that the new Presidential order does not define or clarify the term cryptology sufficiently. This definitional imprecision was viewed as a possible problem for Federal agencies as they attempt to implement the encryption measures.

Another policy concern with the Executive order, while not explicitly discussed in the House report, is its use in lieu of a specific computer security policy. The National Communications Security Committee, chaired by NSA, surveyed the Federal agencies and found that they use the Executive order on Security Classification Policy as the basic policy document in planning and implementing computerized systems.[54] Therefore any problems or deficiences inherent in the Executive order may have an extensive affect on many Federal computer security plans and procedures.

---

[52] U.S. Congress. House. Committee on Government Operations. "The Government's Classification of Private Ideas." House Report No. 96-1540, 96th Congress 2d session, Washington, D.C., U.S. Government Printing Office, 1980. 244 p.

[53] U.S. Congress. House. Committee on Government Operations. "Security Classification Policy and Executive Order 12356." House Report No. 97-731, 97th Congress 2d session, Washington, D.C., U.S. Government Printing Office, 1980.

[54] U.S. Department of Defense. Office of Secretary of Defense. National Communications Security Committee. Computer Security Working Group. Policy Survey Subcommittee. Survey of Federal Computer Security Policies. November 1980. Washington, D.C. 1980. p. 4. Hereafter referred to as U.S. Department of Defense Survey. * * *

III. EXECUTIVE BRANCH RESPONSIBILITIES AND ACTIONS

Responsibilities for Federal information technology management are shared by the individual agency and the central management agencies. For the most part, computer security management mirrors this arrangement except in the handling of classified data, sensitive national security information, and sensitive communications. The responsibility for sensitive and classified communication is shared by the Secretary of Defense, as executive agent for communications security,[55] and the Secretary of Commerce, as executive agent for communications protection.[56] Computerized resources with links to these communication systems are consequently affected. According to some security experts, the Government may be considering reviewing these communication protection functions.

Federal computer security measures derive from both specific statutory requirements and Government directives. For example, statutory requirements such as the Privacy Act of 1974 (title 5 U.S.C. 552a) require protection of records which identify an individual and contain personal information. Other statutory provisions call for maintaining the confidentiality of personal records and limiting dissemination of certain records (for example, census, internal revenue, social security). In addition there are a broad range of laws directed at protecting Government assets.[57] While some of the directives relating to national security are classified, others are stated in Presidential Directives and Office and Management and Budget Circulars. A recent survey by the National Communications Security Committee indicates that many Federal agency computer security policies are based on the Executive order for handling classified data (Executive Order 12356).[58]

A. Executive Branch Problems Cited in GAO and Congressional Reports

According to numerous GAO reports and congressional committee investigations, Federal agency failures to conduct risk assess-

[55] This function, delegated to the National Security Agency [NSA], is described in U.S. Library of Congress. Congressional Research Service. "National Security Agency: Computer-Communication Security Issues." (CRS [White Paper] 83-525 SPR) June 14, 1983. Authored by Louise Giovane Becker. Washington, D.C., 1983. 16 pages.

[56] Presidential Directive 24 [PD-24], a classified document, establishes a national telecommunications protection policy. An unclassified extract indicates that responsiblities for policy are assigned to the Secretary of Defense (subsequently delegated to the Director of the National Security Agency) and the Secretary of Commerce as executive agent for communications protection. Source: U.S. Comptroller General. "Increasing Use of Data Telecommunications Calls for Stronger Protection and Improved Economies." LCD-81-1, Nov. 12, 1980. Washington, D.C., U.S. General Accounting Office, 1980. p. 17.

[57] For example, title 18 U.S.C. 641 (embezzlement and theft prohibition of government property) and title 18 U.S.C. 1343 (wiretapping-penalties for fraudulent obtaining of money or property through the use of wire, radio or televison communications) provide criminal penalties for unlawfully accessing Government records.

[58] U.S. Department of Defense. Survey * * * Op. cit.

24-810 O - 83 - 4

ments and implement controls have endangered some information systems. This section of the report reviews the failure of some Federal agencies to implement security programs; the lack of upper level management support for computer security; difficulties encountered in implementing OMB Circular A–71, Transmittal Memorandum No. 1, and the lack of controls of certain sensitive systems.

1. FAILURE TO IMPLEMENT COMPUTER SECURITY PROGRAMS

Investigations by the General Accounting Office and others indicate that some Federal agencies have been lax in fully protecting computerized resources. In many instances the lack of controls, failure to pinpoint responsibilities, and limited compliance with statutory or regulatory requirements are cited as causing a wide range of abuses. In addition, agency failures to protect certain sensitive record systems make them vulnerable to abuse and may contribute to the erosion of personal freedoms.[59]

In the last two decades there has been a dramatic increase in the use of computers by the Federal Government, but the development of safeguards for these systems has lagged. In addition to limited allocation of resources for computer security, agencies often fail to develop adequate contingency and emergency plans, according to GAO.[60]

GAO also found that agencies have not developed comprehensive computer security programs to address technical, administrative and physical protective measures.[61] Furthermore, agencies have not always placed the computer security function at a sufficiently high level, or with sufficient independence from operational functions to provide the appropriate perspective.[62]

Some of the agencies surveyed by GAO had not established centrally directed computer security programs to provide adequate protection.[63] In addition, GAO found that computer security provisions were often fragmented and restricted to the protection of only some data elements. In one instance a Federal agency did not have a written set of security procedures.[64]

2. LIMITED SUPPORT BY SENIOR MANAGEMENT

Under the Paperwork Reduction Act of 1980 Federal agencies have an opportunity to improve planning coordination and accountability over computer resources. The act requires that a senior official be appointed to aid in coordination of agency information resources. The senior official's office, some experts believe, provides an opportunity to centralize the computer security function. Few agencies, however, have used the law effectively to improve computer security management. For example, the GAO found that the lack of coordination within the Department of the

---

[59] GAO. Automated Systems Security * * * p. i.
[60] U.S. Comptroller General. "Most Federal Agencies Have Done Little Planning for ADP Disasters." AFMD–81–16, Dec. 18, 1980. Washington, D.C., U.S. General Accounting Office, 1980. p. 20.
[61] GAO Automated Systems Security * * * Op. cit., p. iii.
[62] Ibid.
[63] Ibid., p. 10.
[64] Ibid.

Treasury endangers that agency's computer resources.[65] The GAO specifically pointed out that Treasury did not take advantage of the statutory framework to improve computer performance and obtain better control of computer resources.[66]

In some instances controls over automated information systems—specifically those that contain personal, proprietary and other sensitive records [67]—are not fully defined or implemented.[68] Senior management has not always supported internal review functions related to the computer security program.[69] GAO stated that officials responsible for internal reviews indicated that senior management was reluctant to allocate time and resources to assure proper performance of this function.[70] Evidence of limited support by Federal managers, according to GAO, was seen in the: [71]

—Limited resources committed to and used for risk management;
—Failure to define data processing operations in accordance with OPM criteria for personnel security programs;
—Failure to provide reliable contingency and backup hardware and software; and
—Failure to provide an appropriate separation of duties between information security officers and data processing managers.

3. PROBLEMS IN IMPLEMENTATION OF TM-1

The lack of direction and specificity of OMB Circular A-71, Transmittal Memorandum No. 1 [TM-1] is believed by some experts to limit support of agency computer security efforts. A specific stumbling block in implementing TM-1 is the lack of a workable definition of what is a "reasonable level of protection" for Federal information systems.[72]

TM-1 requires each agency to establish controls, but "does not identify the specific controls nor the circumstances under which it is best to use one type of control versus another." [73] Indicative of the confusion regarding TM-1, Federal agencies responding to the survey by the National Communication Security Committee seldom cited TM-1 as the authoritative basis for establishing controls.[74]

TM-1 calls for agencies to perform risk analysis to determine what, if any, are the vulnerabilities of the facility or installation. A GAO evaluation indicated that agencies do not generally use risk analysis techniques, other forms of controls (that is, employee background investigations or contingency planning to insure the availability of backup equipment and software), or systematic reviews.[75]

---

[65] U.S. Comptroller General. "The Treasury Department and Its Bureaus Can Better Plan For and Control Computer Resources." GGD-82-9. Feb. 22, 1982. Washington, D.C., U.S. General Accounting Office, 1980, p. 5.
[66] Ibid., p. 45.
[67] This investigation excluded classified information (for example, national security related data) which is governed by executive orders, National Communication Security directives, and laws such as the Atomic Energy Act of 1954.
[68] GAO. "Federal Information Systems Remain Highly Vulnerable".* * * Op. Cit. p. 1.
[69] Ibid., p. 27.
[70] Ibid.
[71] Ibid., p. 28.
[72] Ibid., p. 9.
[73] Ibid., p. 10.
[74] Ibid
[75] Ibid., pp. 23-24.

A number of other problems with TM-1 were identified by GAO. These include the fact that TM-1 does not translate the broad social goals of privacy (Privacy Act of 1974) and openness in Government (Freedom of Information Act) into design and implementation of systems.[76] In addition, TM-1 does not clarify what information should be classified and what protections are needed. GAO found that TM-1 does not identify when sensitive information should receive the same protections as classified information and therefore may require further clarification.[77] Another difficulty agencies are confronted with is that TM-1 does not give policy direction in securing those systems dependent on telecommunication networks.[78]

4. DIFFICULTIES IN INSTITUTING CONTROLS

The lack controls in financial systems may make them particularly vulnerable to fraud and abuse. For example, the GAO investigation of the Community Services Administration [CSA] indicated problems associated with a lack of internal controls.[79] Specifically, the GAO reported that the Community Services Administration has not conducted sufficient and timely reviews of its automated cash management systems. In addition, deficiencies in certain physical security controls, not directly the responsibility of the Community Services Administration, and the lack of a formal risk analysis review contribute to the lack of security in sensitive finanical systems. GAO's investigation of CSA is just one example. Others include:

—"IRS' Security Program Requires Improvements to Protect Confidentiality of Income Tax Information" (GGD-77-44, July 11, 1977);

—"Flaws in Controls Over the Supplemental Security Income Computerized System Causes Millions in Erroneous Payments" (HRD-79-104, August 9, 1979) and;

—"Solving Social Security's Computer Problems: Comprehensive Corrective Action Plan and Better Management Needed" (HRD-82-19, December 1981).

B. Central Management Agencies

1. OFFICE OF MANAGEMENT AND BUDGET

OMB has overall responsibility for guidance and policy on computer security. This includes the formulation of policies such as:

—OMB Circular A-71, Transmittal memorandum No. 1 [TM-1], "Security of Federal Automated Information Systems."

—OMB Circular A-108, "Responsibilities for Maintenance of Records About Individuals by Federal Agencies."

—OMB Circular A-123, "Internal Controls Systems."

---

[76] Ibid.
[77] Ibid., p. 12.
[78] Ibid.
[79] U.S. Comptroller General. "Weak Financial Controls Make the Community Service Administration Vulnerable to Fraud and Abuse." FGMS-80-73. Aug. 22, 1980. Washington, D.C., U.S. General Accounting Office, 1980.

a. Lack of strong leadership

OMB as the principle central management agency has not provided the strong leadership role needed in executing the Federal computer security program, according to GAO and congressional investigations.[80] Furthermore, OMB has been criticized for not providing the appropriate coordination of responsibility for computer security as required by the Privacy Act of 1974 and implied in the Paperwork Reduction Act of 1980.[81]

b. OMB's organization

The Paperwork Reduction Act of 1980 established OMB's Office of Information and Regulatory Affairs [OIRA]. This office is charged with coordinating Federal information resources management activities. Congressional investigations indicate that OIRA has failed to pursue actively the responsibility required by the law. Another factor in OIRA's lack of support for computer security management may be its organizational structure. OIRA uses a "desk officer" concept in which a single person may be responsible for providing guidance on a broad range of complex subjects, such as paperwork reduction, information systems development, information resource reviews, privacy, as well as computer security. Some observers feel that the lack of specialization of the "desk officers" hampers their ability to deal with complex computer security topics. Finally, critics charge that OMB's guidance in this area has not been precise and consequently does not provide good direction.[82]

2. GENERAL SERVICES ADMINISTRATION

The General Services Administration [GSA] is responsible for the development and enforcement of Federal computer security regulations.[83] GSA's Information Resources Management Division (formerly, Automated Data and Telecommunications Services Division) establishes guidance for other agencies in certain data processing procurement and management areas. GSA's agency reviews have not been directed at evaluating agency compliance with automated information security regulations. Although improving the reviews to aid in determining performance may be of some help, in the past they have not had the scope or direction to be useful for assisting agencies in obtaining a "reasonable level of protection over their information systems," according to GAO.[84]

GAO reported that GSA had issued three revisions to its Government-wide regulation, but has not "taken an adequate role to ensure executive agencies comply with them." [85] Without such follow up, agencies have failed to implement Government-wide in-

---

[80] GAO. "Federal Information Systems Remain Highly Vulnerable. * * *" Op. cit., p. 13.
[81] Ibid.
[82] GAO. "Federal Information Systems Remain Highly Vulnerable * * *" Op. cit.
[83] Computer security related regulations include: Federal Procurement Management Regulation (FPMR 101-35.3), security of Federal ADP [Automatic Data Processing] and telecommunications (FPMR 101-36.7) environment and physical security, and Federal Procurement Regulation (FPR 1-4.11) on security requirements for Federal agencies and Government contractors.
[84] GAO. "Federal Information Systems Remain Highly Vulnerable * * *" Op. cit., p. 20.
[85] Ibid., p. 21.

formation security policies, principles, standards, and guidelines appropriately.[86]

GAO previously claimed that GSA had failed to coordinate computer security policies, guidance, and standards. They stated that the lines of coordination between central management agencies have not been entirely clear nor effective.[87] However, at present some efforts are being made to remedy this situation.[88]

3. OTHER CENTRAL MANAGEMENT AGENCIES

The Office of Personnel Management [OPM] is responsible for providing guidance with regard to background checks of personnel involved with computers. GAO specifically criticized the narrow definition of employees requiring clearances. Failure to provide appropriate employee background checks for personnel associated with certain information systems remains a problem. Another area in which GAO found that OPM did not provide sufficient guidance was in the treatment of contractor personnel.[89]

The National Bureau of Standards Institute for Computer Science and Technology [ICST] provides guidelines and standards in support of Federal agency computer security efforts.[90] Cuts in funding of the Institute's programs and debates regarding the organizational placement of the Institute may have limited ICST computer security program initiatives. In addition, it is not clear to what extent coordination exists between ICST programs and certain initiatives within the Department of Defense, such as the DOD Computer Security Center. Given the dimension of Federal computer security concerns, it may be important to enhance the ICST computer security programs.

C. Department of Defense

The Department of Defense [DOD] has responsibility for certain government-wide computer security functions as well as those within DOD. The National Security Agency has been delegated some of the responsibility to protect certain information and communications from unwanted dissemination. Beginning in the late 1970's the Department of Defense began a series of initiatives in support of computer security technologies research and development. For example, the recently established DOD Computer Security Center, operated by the National Security Agency, is using a more open approach to development and support of computer security technology research than other NSA programs have in the past. This approach, a significant departure from other NSA operations, is designed to develop a working partnership between industry and NSA to enhance computer security features of certain systems. Concerns have been raised about whether it is consistent with NSA policy to maintain such a level of openness. In addition,

---

[86] Ibid.

[87] Ibid., p. 19.

[88] For example GSA has begun to coordinate its regulations on Federal computer security standards and guidelines.

[89] Ibid., p. 20–21.

[90] For example the Data Encryption Standard [DES], an NBS supported standard, is in use in those Federal agencies which require protection of sensitive but not classified data.

questions have been asked about the possible conflicts between the Center and other NSA or Federal programs.

On the other hand a legacy of too few open exchanges and limited information transfers has sometimes restricted universal acceptance of other NSA computer security related decisions. Because NSA has not always been able to share the technological basis of certain decisions, there has been an appearance that there may be little scientific basis for these decisions. More recently, NSA has recognized that computer security technology cannot realistically be developed in a vacuum and the agency is initiating a dialog with those in industry and academia on development of appropriate technology.[91]

A critical problem remains the direction or approach of computer security technology. At present a major focus of the DOD Computer Security Center is to promote the development of "trusted" computers.[92] While this goal is of use in DOD, there is less agreement on its applicability to the other agencies of Government or the private sector.

Critics also have expressed reservations regarding the development of computer security technology dominated by one perspective; namely NSA. Another problem is the potential lack of coordination between other civilian Government agencies and the Department of Defense in supporting computer security. For example, it is not clear what coordination exists between the Center's evaluation program and the National Bureau of Standard's computer certification program. However, since the DOD center is in a start-up phase more experience may be needed to judge appropriately the merits of the present approach and the direction being pursued.

---

[91] U.S. Library of Congress. Congressional Research Service. "Computer Security: An Overview of National Concerns and Challenges." Op. cit.

[92] A "trusted" computer system is one that employs sufficient hardware and software integrity measures to allow its use in simultaneous processing of multilevels of classified or sensitive information. An ideal "trusted" computer system, containing unclassified, secret, top secret, and so forth, information could be accessed by users with different levels of security clearance and, would allow safe handling of the data.

IV. APPENDICES

Computer Security and Computer-Related Crime:

Selected References, 1967-1983

Preface

This bibliography has been prepared to supplement the information provided in the committee print. The intent is to provide the reader with an understanding of the scope and nature of the literature on various aspects of computer-related crime.

The references to articles and monographs have for the most part been selected from the computerized data base maintained by the Library Services Division of the Congressional Research Service. Other sources searched for additional information included commercial data bases, published indexes to periodical literature and government reports, and the catalogs of the Library of Congress.

Citations to items in the classified collections of the Library of Congress are provided with call numbers. Items designated LAW are unclassified works located in the Law Library. Journal articles are provided with call numbers for the bound volume location regardless of whether the issues were bound at the time that they were cited. Unbound issues will be found in the Newspaper and Current Periodical Room or the Law Library.

Louise Becker provided invaluable assistance in the selection of material from the plethora of documents available on the topic of computer security. Richard Gigax, Head of the Subject Specialization Section, Library Services Division, provided time and experience to assure that the contents and style followed bibliographic standards.

Charles P. Dove
Senior Bibliographer, Science
Library Services Division
March 4, 1983

I. Computer Security

Abouchar, Roger J. Threats to EFT systems. Magazine of bank administration, v. 54, Apr. 1980: 28, 30-33. HG1501.A87, v. 54

Abrams, Marshall D., and others. Tutorial on computer security and integrity. [New York, Institute of Electrical and Electronics Engineers] available from IEEE Computer Society, 1977. 1 v. (various pagings) HF5548.2.T86

Becker, H. J. Security in an electronic fund transfer system. Information privacy, v. 2, Sept. 1980: 185-189. K3263.A13I53, v. 2

Bernard, Robert. Breaching system security. IEEE spectrum, v. 19, June 1982: 24-31. AS36.R28, v. 19

Branstad, D. K. Security of computer communication. IEEE Communications Society magazine, v. 16, Nov. 1978: 33-40. TK5101.A1I139, v. 16

Carroll, John Millar. Data base and computer systems security. Wellesley, Mass, Q.E.D. Information Sciences, 1976. 60 p. QA76.9A25C37

Coates, Joseph F. The future of computer data security. Vital speeches of the day, v. 48, Feb. 15, 1982: 380-284. PN6121.V5, v. 48

Cohn, Arnold M. Total information security. Journal of systems management, v. 33, Apr. 1, 1982: 14-17. HD28.S953, v. 33

Green, Gion. Introduction to security. 3d ed. Boston, Butterworth, 1981. 395 p. HV8290.G74 1981

Heinrich, Frank. The Network Security Center: a system level approach to computer network security. [Washington] U.S. National Bureau of Standards [for sale by the Supt. of Docs., U.S. Govt. Print. Off.] 1978. 55 p. (NBS special publication 500-21, v. 2)

Hondius, F. W. Computers: data privacy. IEEE spectrum, v. 17, Mar. 1980: 67-70. AS36.R28, v. 17

Hsiao, David K., Douglas S. Kerr, and Stuart E. Madino. Computer security. New York, Academic Press, 1979. 299 p. QA76.9.A25H74

International Business Machines Corporation. Data security and data processing. White Plains, N.Y., 1974. 7 v. HF5548.2.I458 1974

International Computer Software & Applications Conference, 2d, Chicago, 1978. COMPSAC 78: the IEEE Computer Society's Second International Computer Software & Applications Conference; proceedings. New York, Institute of Electrical and Electronics Engineers, 1978. 832 p. QA76.6.I546 1978

Keplinger, Michael S. Computer software--its nature and its protection. Emory law journal, v. 30, spring 1981: 483-512. K10.Q885, v. 30

McIsaac, Don. Introduction to computers: security problems and considerations. Assets protection, v. 6, Nov.-Dec. 1981: 13-20. HV8290.A8, v. 6

Menkus, Belden. Management's responsibilities for safeguarding information. Journal of systems management, v. 27, Dec. 1976: 32-38. HD28.S953, v. 27

Nielsen, N. R., and B. Ruder. Computer system integrity vulnerability. Information privacy, v. 2, Jan. 1980: 21-25. K3263.A13I53, v. 2

Northup, Ernest H. Bank cards vs. the underworld. Banking, v. 67, Sept. 1975: 66, 68, 70, 73. HG1501.B6, v. 67

Nycum, Susan Hubbell. Security for electronic funds transfer systems. University of Pittsburg law review, v. 37, summer 1976: 709-724.
K25.N7, v. 37

Orceyre, Michel J., and Robert H. Courtney, Jr. Considerations in the selection of security measures for automatic data processing systems: contributed to the Federal Information Processing Standards Task Group 15-Computer Systems Security. Washington, U.S. National Bureau of Standards, for sale by the Supt. of Docs., U.S. Govt. Print. Off, 1978. 1 v. (various pagings)
QC100.U57 no. 500-33

Parker, Donn B. Computer security management. Reston, Va., Reston Pub. Co., 1981. 308 p. QA76.9.A25P38

Petersen, Harold Emanuel, and R. Turn. System implications of information privacy. [Santa Monica, Rand Corp.] 1967. 40 p. (Rand Corporation. Paper P-3504)
A836.R28 no. 3504

Pritchard, J. Computer security and unionization. Information privacy, v. 2, Mar. 1980: 69-74. K3263.A13I53, v. 2

Ross, Steven. Who is the data security officer? Magazine of Bank Administration, v. 58, Oct. 1982: 52, 54, 56, 58.

Ruder, Brian, and J. D. Madden. An analysis of computer security safeguards for detecting and preventing intentional computer misuse. Washington, U.S. National Bureau of Standards, for sale by the Supt. of Docs., U.S. Govt. Print. Off., 1978. 1 v. (various pagings) (NBS special publication 500-25)

Shurn, Peter J. Electronic funds transfer systems: a need for new law? New England law review, v. 12, summer 1976: 111-134. LAW

Squires, T. People and security: an introduction. [Manchester, Eng.] National Computing Centre [1980] 61 p. HF5548.2.S767

Talbot, J. R. Management guide to computer security. New York, Wiley, 1981. 180 p. HF5548.2.T25

Turn, R., R. Frederickson, and D. Hollingworth. Data security research at the Rand Corporation: description and commentary. [Santa Monica, Calif., Rand Corp.] 1972. 23 p. (Rand Corporation. Paper P-4914)
A836.R28 no. 4914

U.S. Congress. Senate. Committee on Government Operations. Problems associated with computer technology in Federal programs and private industry: computer abuses. Washington, U.S. Govt. Print. Off., 1976. 448 p.
JK468.A8U47 1976

——— Staff study on computer security in Federal programs. Washington, U.S. Govt. Print. Off., 1977. 298 p. JK468.A8U47 1977
At head of title: 95th Congress. 1st session. Committee print.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Criminal Justice. Computer Systems Protection Act of 1979, S. 240. Hearing, 96th Congress, 2d session, on S. 240. Feb. 28, 1980. Washington, U.S. Govt. Print. Off., 1980. 179 p. KF26.J8377 1980f
"Serial no. 96-75"

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Criminal Laws and Procedures. Federal Computer Systems Protection Act. Hearings, 95th Congress, 2d session, on S. 1766. June 21-22, 1978. Washington, U.S. Govt. Print. Off., 1979. 213 p. KF26.J838 1978b

U.S. General Accounting Office. Automated systems security--Federal agencies should strengthen safeguards over personal and other sensitive data; report to the Congress by the Comptroller General of the United States. Washington, 1979. 74 p. JK468.A8U5 1979
"LCD-78-123, Jan. 23, 1979"

----- Managers need to provide better protection for Federal automatic data processing facilities, multiagency; report to the Congress by the Comptroller General of the United States. Washington, 1976. 62 p. JK468.A8U5 1976b
"FGMSD-76-40, May 10, 1976"

----- Most Federal agencies have done little planning for ADP disasters; report to the Congress by the Comptroller General of the United States. Washington, 1980. 20 p.
"AFMD-81-16, Dec. 18, 1980"

----- Procedures to safeguard Social Security beneficiary records can and should be improved; report by the Comptroller General of the United States. Washington, 1978. 41 p.
"HRD-78-116, June 5, 1978"

----- Safeguarding taxpayer information: an evaluation of the proposed computerized tax administration system, Office of Education, Department of Health, Education and Welfare; report to the Congress by the Comptroller General of the United States. Washington, 1977. 44 p. HJ3252.U57 1977
"LCD-76-115, Jan. 17, 1977"

U.S. National Bureau of Standards. Computer security guidelines for implementing the Privacy Act of 1974. [Washington, For sale by the Supt. of Docs., U.S. Govt. Print. Off.] 1975. 20 p. (Federal information processing standards publications. FIPS pub. 41)

----- Guidelines for automatic data processing physical security and risk management; category: ADP operations, subcategory: computer security. [Washington, For sale by the Supt. of Docs., U.S. Govt. Print. Off.] 1974. 92 p. (Federal information processing standards publication. FIPS pub. 31)

Vulnerability of computerised society. OECD observer, no. 114, Jan. 1982: 36-38. HC240.A102

II. Crime

Ball, Leslie D. Computer crime. Technology review, v. 58, Apr. 1982: 21-27, 30. T171.MH, v. 58

Becker, Jay J. The investigation of computer crime: an operational guide to white collar crime enforcement. Washington, U.S. Law Enforcement Assistance Administration, for sale by the Supt. of Docs., U.S. Govt. Print. Off., 1980. 73 p. HV8079.W47B4 1980

Bequai, August. Organized crime in the computer arena. Police chief, v. 45, Oct. 1978: 24, 26, 28-29. HV7551.P5, v. 45

----- A survey of fraud and privacy obstacles to the development of an electronic funds transfer system. Catholic University law review, v. 25, summer 1976: 766-800. K3.A79, v. 25

Boockholdt, J. L., and Jerome S. Horvitz. Prosecution of computer crime. Journal of systems management, v. 29, Dec. 1978: 6-11. HD38.S953, v. 29

Friedman, Robert. The Dalton Gang's computer caper. New York, v. 13, Dec. 8, 1980: 65-75. F128.1.N4, v. 13

Goldberg, Leslie L. Computers and crime. Telecommunications, v. 14, May 1980: 19-20, 22, 24, 26. TK5101.A1T32, v. 14

Haggman, Bertil. The vulnerable modern industrial society. Jerusalem journal of international relations, v. 3, summer 1978: 1-18. JX18.J47, v. 3

Henderson, Bruce, and Jeffrey Young. The heist. Esquire, v. 95, May 1981: 36-40, 42, 45, 47. AP2.E845, v. 95

Jacobson, R. A perfect computer crime. Information privacy, v. 1, Mar. 1979: 160-163. K3263.A13I53, v. 1

Krauss, Leonard K., and Aileen MacGahan. Computer fraud and countermeasures. Englewood Cliffs, N.J., Prentice-Hall, 1979. 309 p. HV6773.K7

Leepson, Marc. Computer crime. [Washington, Editorial Research Reports] 1978. 20 p. (Editorial research reports, 1978, v. 1, no. 1) H35.E35 1978, v. 1

Parker, Donn B. Crime by computer. New York, Scribner, 1976. 308 p. HV6773.P37

Peterson, Ivars. Computer crime: insecurity in numbers. Science news, v. 122, July 3, 1982: 12-14. Q1.S76, v. 122

Sokolik, Stanley Lewis. Computer crime: its setting and the need for deterrent legislation. Springfield, Data Information Systems Commission, Illinois General Assembly, 1979. 72 p. KFI1768.C65S64

The Spreading danger of computer crime. Business week, no. 2684, Apr. 20, 1981: 86-92. HF5001.B89

SRI International. Computer crime: criminal justice resource manual. [Washington] National Criminal Justice Information and Statistics Service, Law Enforcement Assistance Administration, U.S. Dept. of Justice [for sale by the Supt. of Docs., U.S. Govt. Print. Off.] 1979. 392 p. HV6773.S18 1979

Sugarman, Robert. On foiling computer crime. IEEE spectrum, v. 16, July 1979: 31-41. TK1.I15, v. 16

Swanson, C. R., and Leonard Territo. Computer crime: dimensions, types, causes, and investigation. Journal of police science and administration, v. 8, no. 3, 1980: 304-311. HV7551.J68, v. 8

Theft in the health care industry. Germantown, Md., Aspen Systems Corp., 1978. 99 p. (Topics in health care financing, v. 5, no. 20095-3814) RA969.95.T48

U.S. General Accounting Office. Computer-related crimes in Federal programs; report to the Congress by the Comptroller General of the United States. Washington, 1976. 24 p. HV6773.U55 1976
"FGMSD-76-27, Apr. 27, 1976"

------ Federal information systems remain highly vulnerable to fraudulent, wasteful, abusive, and illegal practices; report. Washington, 1982. 29 p.
"MASAD-82-18, Apr. 21, 1982"

------ Weak financial controls make the Community Services Administration vulnerable to fraud and abuse; report to the Congress by the Comptroller General of the United States. Washington, 1980. 100 p.
"FGMSD-80-73, Aug. 22, 1980"

U.S. Library of Congress. Science Policy Research Division. Computer crime and security [by] Louise Becker. [Washington] 1983. 3 p. (Issue brief IB80047)
Regularly updated.
For Congressional use only.

III. Innovation

Hemphill, Charles F. Modern security methods. Englewood Cliffs, N.J., Prentice-Hall, 1979. 300 p. HV8290.H44

----- Security safeguards for the computer [by] Charles F. Hemphill and Robert D. Hemphill. New York, AMACOM, 1979. 38 p. (An AMA management briefing) HF5548.2.H4477

Lobel, Jerome. Planning a secure system. Journal of systems management, v. 27, July 1976: 14-19. HD28.S953, v. 27

National Telecommunications Conference, Birmingham, Ala., 1978. NTC '78 record. New York, Institute of Electrical and Electronics Engineers, 1978. 340 p. TK5101.A1N374 1978

Perry, William E. Management guide to computer security and control. New York, Wiley, 1980. 207 p. HF5548.2.P4728

Tutorial on computer security and integrity. Long Beach, Calif., IEEE Computer Society, 1977. 450 p. HF5548.2.T86

U.S. Congress. Senate. Committee on Governmental Affairs. Paperwork Reduction Act of 1980; report to accompany S. 1411 to improve the economy and efficiency of the government and the private sector by improving Federal information policymaking, and for other purposes, together with additional views. Washington, U.S. Govt. Print. Off., 1980. 111 p. (96th Congress, 2d session. Senate. Report no. 96-930)

U.S. General Accounting Office. Continued use of costly, outmoded computers in Federal agencies can be avoided; report to the Congress by the Comptroller General of the United States. Washington, 1980. 61 p.
"AFMD-81-9, Dec. 15, 1980"

----- Conversion: a costly, disruptive process that must be considered when buying computers; report to the Chairman, Committee on Appropriations, House of Representatives, by the Comptroller General of the United States. Washington, 1980. 78 p.
"FGMSD-80-35, June 3, 1980"

----- Electronic funds transfer--its potential for improving cash management in government; report to the Congress by the Comptroller General of the United States. Washington, 1980. 29 p.
"FGMSD-80-80, Sept. 19, 1980"

----- Federal electrical emergency preparedness is inadequate; report to the Congress by the Comptroller General of the United States. Washington, 1981. 40 p.
"EMD-81-50, May 12, 1981"

----- Improvements needed in managing automated decisionmaking by computers throughout the Federal Government; report to the Congress by the Comptroller General of the United States. Washington, 1976. 72 p. JK468.A8U5 1976a
"FGMSD-76-5, Apr. 23, 1976"

----- Stronger management of EPA's information resources is critical to meeting program needs; report to the Congress by the Comptroller General of the United States. Washington, 1980. 73 p.
"CED-80-18, Mar. 10, 1980"

——— Wider use of better computer software technology can improve management control and reduce costs; report to the Congress by the Comptroller General of the United States. Washington, 1980. 57 p. JK468.A8R5 1980
"FGMSD-80-38, Apr. 29, 1980"

——— The World Wide Military Command and Control System—evaluation of vendor and Department of Defense comments; report to the Congress by the Comptroller General of the United States. Washington, 1980. 70 p.
"LCD-80-22A, June 30, 1980"

——— The World Wide Military Command and Control System—major changes needed in its automated data processing management and direction; report to the Congress by the Comptroller General of the United States. Washington, 1979. 103 p.
"LCD-80-22, Dec. 14, 1979"

U.S. Library of Congress. Science Policy Research Division. Federal information management policy: critical directions [by] Louise Becker. Washington, 1980. 179 p. (Report no. 80-143 SPR)

Walsh, Myles E. Software security. Journal of systems management, v. 32, Oct. 1981: 6-13. HD28.S953, v. 32

IV. Audits

Andersen, R. E. EDP auditing in the 1980s, or the vanishing paper trail. In Computer Performance Evaluation Users Group (CPEUG): proceedings of the sixteenth meeting held at Orlando, Fla., Oct. 20-23, 1980. Washington, U.S. National Bureau of Standards, 1980. p. 23-30. (NBS special publication 500-65)

Audit and evaluation of computer security: proceedings of the NBS invitational workshop, held at Miami Beach, Fla., Mar. 22-24, 1977. Washington, U.S. National Bureau of Standards, for sale by the Supt. of Docs., U.S. Govt. Print. Off., 1977. 256 p. (NBS special publication 500-19)
QC100.U57 no. 500-19

Audit and evaluation of computer security II: system vulnerabilities and controls; proceedings of the NBS invitational workshop, held at Miami Beach, Fla., Nov. 28-30, 1978. [Washington] U.S. National Bureau of Standards, for sale by the Supt. of Docs., U.S. Govt. Print. Off. [1980] 250 p. (NBS special publication 500-57) QC100.U57 no. 500-57

Browne, Peter. Security checklist for computer center self-audits. Washington, AFIPS Press, 1979. 189 p. HF5548.2.P32 1979

Engel, Norman L., and Paul W. Howerton. Computer security, a management audit approach. New York, AMACOM, 1980. 264 p. HF5548.2.E53

Macchiaverna, Paul R. Auditing corporate data—processing activities. New York, Conference Board, 1980. 85 p. (The Conference Board. Report no. 776)
HF5548.2.M213

U.S. General Accounting Office. Computer auditing in the executive departments: not enough is being done; report to the Congress by the Comptroller General of the United States. Washington, 1977. 54 p.
JK468.A8U5 1977a
"FGMSD-77-82, Sept. 28, 1977"

——— GAO findings on Federal internal audit—a summary; report by the Comptroller General of the United States. Washington, 1980. 47 p.
"FGMSD-80-39, May 27, 1980"

----- New methods needed for checking payments made by computers; report to the Congress by the Comptroller General of the United States. Washington, 1977. 47 p.
"FGMSD-76-82, Nov. 7, 1977"

V. Encryption

Conference on Computer Security and the Data Encryption Standard, Gaithersburg, Md., 1977. Computer science & technology: computer security and the Data Encryption Standard. Washington, U.S. National Bureau of Standards, for sale by the Supt. of Docs., U.S. Govt. Print. Off., 1978. 125 p. (NBS special publication 500-27)

Kahn, D. Cryptology goes public. IEEE communications magazine, v. 18, Mar. 1980: 19-20. TK5101.A1I139, v. 18
Formerly IEEE Communications Society magazine.

Kolata, Gina Bari. Computer encryption and the National Security Agency connection. Science, v. 197, July 29, 1977: 438-440. Q1.S35, v. 197

Konheim, Alan G. Cryptography, a primer. New York, Wiley, 1981. 432 p. Z103.K66

Morris, R. The data encryption standard retrospective and prospects. IEEE Communications Society magazine, v. 16, Nov. 1978: 11-14. TK5101.A1I139, v. 16

Murray, T. J. Cryptographic transformation as a data security tool. In Joint Engineering Management Conference, 26th, Denver, 1978. Engineering management in the computer age. New York, Institute of Electrical and Electronics Engineers, 1978. p. 146-148. TA190.J64 1979

Peterson, Ivars. Cryptology and national security. [Columbia] School of Journalism, University of Missouri at Columbia, 1981. 8 p. (Missouri. University at Columbia. Freedom of Information Center. Report no. 442) KF4774.A7

----- Whom do you trust? Science news, v. 120, Sept. 26, 1982: 205-206. Q1.S76, v. 120

Popek, G. J., and C. S. Kline. Encryption and secure computer networks. Computing surveys, v. 11, Dec. 1979: 331-356. QA76.5.C617, v. 11

U.S. Congress. House. Committee on Government Operations. The government's classification of private ideas; thirty-fourth report together with additional views. Washington, U.S. Govt. Print. Off., 1980. 244 p. (96th Congress, 2d session. House. Report no. 96-1540)

U.S. Congress. Senate. Select Committee on Intelligence. Unclassified summary: involvement of NSA in the development of the data encryption standard; staff report. Washington, U.S. Govt. Print. Off., 1978. 4 p.
At head of title: 95th Congress, 2d session. Committee print.

U.S. General Accounting Office. Continuing problems in DOD's classification of national security information; report to the Congress by the Comptroller General of the United States. Washington, 1979. 35 p.
"LCD-80-16, Oct. 26, 1979"

Zeidler, Howard M. Digital data encryption. Menlo Park, Calif., SRI International, 1979. 20 p. (Business Intelligence Program. Guidelines, no. 1044)

VI. International Data Flow

Epperson, G. Michael. Contracts for transnational information services: securing equivalency of data protection. Harvard international law journal, v. 22, winter 1981: 157-175. JX1.H37, v. 22

Evans, A. C. Data protection in Europe. Journal of world trade law, v. 15, Mar.-Apr. 1981: 150-158. K10.09, v. 15

——— European data protection law. American journal of comparative law, v. 29, fall 1981: 571-582. LAW

Kirby, M. D. Developing international rules to protect privacy. Law and computer technology, v. 12, third quarter 1979: 53-62. LAW

Organization for Economic Cooperation and Development. Guidelines on the protection of privacy and transborder flows of personal data. Paris, 1981. 41 p.

——— Policy issues in data protection and privacy: concepts and perspectives. [Paris, 1976] 324 p. (OECD information studies, 10) JC597.073 1976
"Proceedings of the OECD seminar 24th to 26th of June 1974."

——— Towards central government computer policies: data development and international dimensions. [Paris, 1973] 215 p. (OECD information studies, 6) JF1525.A8974 1973a

——— Transborder data flows and the protection of privacy. Paris, 1979. 335 p. QA76.9.A25896 1977

Organization for Economic Cooperation and Development. Panel on Policy Issues of Computer/Telecommunications Interaction. Computers and telecommunications: economic, technical and organizational issues. Paris, 1973. 222 p. (OECD information studies, 3) TK5102.5.0247 1973

Organization for Economic Cooperation and Development. Working Party on Information, Computer, and Communications Policy. Policy implications of data network developments in the OECD area. Paris, sold by OECD Publications and Information Centre, 1980. 206 p. (Information, computer, communications policy, 3) QA76.0715 1980

Rooms, P. L. P., and J. Dexter. Problems of data protection law for private multinational communication networks. Computer networks, v. 3, June 1979: 205-214. TK5105.5.C647, v. 3

Serwatynski, W. Transborder data flow: a global view. Information privacy, v. 1, Jan. 1979: 133-136. K3263.A13I53, v. 1

Schick, Joseph E., Jr. Transborder data flow. Law and computer technology, v. 11, no. 3, 1978: 62-74. LAW

Symposium on Transborder Data Flows and the Protection of Privacy, Vienna, Austria, 1977. Proceedings. Paris, Organization for Economic Cooperation and Development, 1979. 335 p. QA76.9.A25S96 1979

Transborder data flows: concerns in privacy protection and free flow of information. Arlington, Va., American Federation of Information Processing Societies, 1979. 2 v. K3264.C65T7

U.S. Congress. House. Committee on Government Operations. International information flow: forging a new framework; thirty-second report together with additional views. Washington, U.S. Govt. Print. Off., 1980. 61 p. (96th Congress, 2d session. House. Report no. 96-1535)

BEST COPY AVAILABLE

U.S. Congress. House. Committee on Government Operations. Government Information and Individual Rights Subcommittee. International data flow. Hearings, 96th Congress, 2d session. Washington, U.S. Govt. Print. Off., 1980. 843 p. KF27.G6628 1980
Hearings held Mar. 10-Apr. 21, 1980.

Veith, R. H. Information and transborder data flow: the question of social impact. Journal of the American Society for Information Science, v. 31, Mar. 1980: 105-110. Z1007.A477, v. 31

VII. Privacy

Armer, Paul. Computer technology and surveillance. Computers and people, v. 24, Sept. 1975: 8-11. TJ212.C58, v. 24

Aronoff, Stanley J. 1984--only 11 years away. State government, v. 46, spring 1973: 66-75. JK2403.S7, v. 46

Association for Computing Machinery. Los Angeles Chapter. Ombudsman Committee on Privacy. Privacy, security, and the information processing industry. New York, 1976. 187 p. JC599.U5A77 1976

Computer abuse. New York, Practising Law Institute, 1975. 208 p. (Litigation course handbook series no. 77) KF390.5C6C6

Controversy over Federal "data banks." Congressional digest, v. 50, Oct. 1971: whole issue. JK1.C15, v. 50

Dalal, Jagdish R. Computers and the future. Journal of systems management, v. 32, Aug. 1981: 17-21. HD28.S953, v. 32

DeWeese, J. Taylor. Giving the computer a conscience. Harper's magazine, v. 247, Nov. 1973: 14, 16-17. AP2.H3, v. 247

Koehn, Hank E. Privacy, our problem for tomorrow. Journal of systems management, v. 24, July 1973: 8-10. HD28.S953, v. 24

Laudon, Kenneth C. Privacy and Federal data banks. Society, v. 17, Jan.-Feb. 1980: 50-56. H1.T72, v. 17

Linowes, David F. Must personal privacy die in the computer age? American Bar Association journal, v. 65, Aug. 1979: 1180-1184. LAW

Lundell, E. Drake, and Marguerite Zientara. Innocent join the guilty in police police computer. New scientist, v. 61, Feb. 28, 1974: 534-535. Q1.N52, v. 61

Marchand, Donald A. The politics of privacy, computers, and criminal justice records: controlling the social costs of technological change. Arlington, Va., Information Resources Press, 1980. 433 p. HV936.A8M28

McLuhan, Marshall, and Bruce Powers. Electronic banking and the death of privacy. Journal of communication, v. 31, winter 1981: 164-169. P87.J6, v. 31

National Academy of Sciences, Washington, D.C. Project on Computer Databanks. Databanks in a free society: computers, record-keeping, and privacy; report [by] Alan F. Westin, project director, and Michael A. Baker, assistant project director. New York, Quadrangle Books, 1972. 522 p. JC599.U5N28 1972

Parker, Donn B. Ethical conflicts in computer science and technology. Arlington, Va., AFIPS Press, 1979. 201 p. QA76.9.M65P37

——— Preserving personal privacy in business [by] Donn B. Parker and Brian Ruder. Menlo Park, Calif., SRI International, 1976. 12 p. (Business Intelligence Program. Guidelines, no. 1005) JC599.U5P37

Renninger, Clark R., ed. Approaches to privacy and security in computer systems. [Washington] U.S. National Bureau of Standards, for sale by the Supt. of Docs., U.S. Govt. Print. Off., 1974. 71 p. (NBS special publication 404) QC100.U57 no. 404
"Proceedings of a conference held at the National Bureau of Standards, March 4-5, 1974."

——— Government looks at privacy and security in computer systems; a summary of a conference held at the National Bureau of Standards, Gaithersburg, Maryland, November 19-20, 1973. R. Clark Renninger and Dennis K. Branstad, editors. Washington, U.S. National Bureau of Standards, for sale by the Supt. of Docs., U.S. Govt. Print. Off., 1974. 37 p. (NBS technical note 809) QC100.U5753 no. 809

Rosenberg, Jerry Martin. The death of privacy. New York, Random House, 1969. 236 p. JC599.U5R64

Rule, James, and others. The politics of privacy: planning for personal data systems as powerful technologies. New York, Elsevier, 1980. 212 p. JC596.2.U5P64

SEARCH Group. Standards for security and privacy of criminal justice information. Sacramento, Calif., 1978. 54 p. (Its Technical report no. 13 rev.) Z699.5.C7S4 1977

Skelly, Stephen J. Balancing privacy and efficiency in an electronic world. Law and computer technology, v. 12, second quarter 1979: 38-49. LAW

Sorkin, Michael. The FBI's big brother computer. Washington monthly, v. 4, Sept. 1972: 24-30. E838.W37, v. 4

Symposium on Security and Privacy, Oakland, Calif., 1980. Proceedings. Long Beach, Calif., IEEE Computer Society, 1980. 167 p. QA76.9.A25S95 1980

Turn, R. A brief history of computer privacy/security research at Rand. Santa Monica, Calif., Rand Corp., 1972. 8 p. (Rand Corporation. Paper P-4798) AS36.R28 no. 4798

——— Privacy and security in centralized vs. decentralized databank systems [by] R. Turn, Norman Z. Shapiro, and Mario L. Juncosa. Santa Monica, Calif., Rand Corp., 1975. 31 p. (Rand Corporation. Paper P-5346) AS36.R28 no. 5346

U.S. Congress. Senate. Committee on Government Operations. Ad Hoc Subcommittee on Privacy and Information Systems. Privacy: the collection, use, and computerization of personal data. Joint hearings before the Ad Hoc Subcommittee on Privacy and Information Systems of the Committee on Government Operations and the Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, Ninety-third Congress, second session. June 18, 19, and 20, 1974. Washington, U.S. Govt. Print. Off., 1974. 2 v. KF26.G6586 1974

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Federal data banks and constitutional rights; a study of data systems on individuals maintained by agencies of the United States Government: summary and conclusions. Washington, U.S. Govt. Print. Off., 1974. 53 p. JC599.U5U53 1974

U.S. General Accounting Office. Challenges of protecting personal information in an expanding Federal computer network environment; report to the Congress by the Comptroller General of the United States. Washington, 1978. 47 p. JC599.U5U56 1978
"LCD-76-102, Apr. 28, 1978"

------ Increasing use of data telecommunications calls for stronger protection and improved economies; report by the Comptroller General of the United States. Washington, 1980. 69 p.
"LCD-81-1, Nov. 12, 1980"

------ VA's new computer system has potential to protect privacy of individuals claiming benefits; report. Washington, 1978. 29 p.
"HRD-78-135, July 17, 1978"

U.S. National Criminal Justice Information and Statistics Service. Privacy and security planning instructions: criminal justice information systems. [Washington] 1976. 63 p.

U.S. Privacy Protection Study Commission. Personal privacy in an information society. Washington, For sale by the Supt. of Docs., U.S. Govt. Print. Off., 1977. 654 p. JC599.U5U58 1977

Ware, Willis H. Computer privacy and computer security. Santa Monica, Calif., Rand Corp., 1974. 5 p. (Rand Corporation. Paper P-5354)
AS36.R28 no. 5354

------ Data banks, privacy, and society. Santa Monica, Calif., Rand Corp., 1973. 11 p. (Rand Corporation. Paper P-5131) AS36.R28 no. 5131

------ Security and privacy in computer systems. [Santa Monica, Calif., Rand Corp.] 1967. 28 p. (Rand Corporation. Paper P-3544)
AS36.R28 no. 3544

Westin, Alan F. Computer science & technology: computers, personnel administration, and citizen rights. [Washington] U.S. National Bureau of Standards [for sale by the Supt. of Docs., U.S. Govt. Print. Off.] 1979. 439 p. (NBS special publication 500-50) QC100.U57 no. 500-50

Workshop on Computers and Privacy in the Next Decade, Pacific Grove, Calif., 1979. Computers and privacy in the next decade; proceedings. Sponsored by the Special Committee on the Right to Privacy of the American Federation of Information Processing Societies. New York, Academic Press, 1980. 215 p. JC596.2.U5C65

97TH CONGRESS
1ST SESSION

H. R. 3970

To amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

IN THE HOUSE OF REPRESENTATIVES

JUNE 18, 1981

Mr. NELSON introduced the following bill; which was referred to the Committee on the Judiciary

---

A BILL

To amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Federal Computer Systems Protection Act of 1981".

SEC. 2. The Congress finds that—

(1) computer-related crime is a growing problem in the Government and in the private sector;

BEST COPY AVAILABLE

(2) such crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime;

(3) the opportunities for computer-related crimes in Federal programs, in financial institutions, and in computers which operate in or use a facility of interstate commerce through the introduction of fraudulent records into a computer system, unauthorized use of computer facilities, alteration or destruction of computerized information files, and stealing of financial instruments, data, or other assets, are great;

(4) computer-related crime directed at computers which operate in or use a facility of interstate commerce has a direct effect on interstate commerce; and

(5) the prosecution of persons engaged in computer-related crime is difficult under current Federal criminal statutes.

SEC. 3. (a) Chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following new section:

"§ 1028. Computer fraud and abuse

"(a) Whoever uses, or attempts to use, a computer with intent to execute a scheme or artifice to defraud, or to obtain property by false or fraudulent pretenses, representations, or

BEST COPY AVAILABLE

promises, or to embezzle, steal, or knowingly convert to his use or the use of another, the property of another, shall, if the computer—

"(1) is owned by, under contract to, or operated for or on behalf of:

"(A) the United States Government; or

"(B) a financial institution;

and the prohibited conduct directly involves or affects the computer operation for or on behalf of the United States Government or financial institution; or

"(2) operates in, or uses a facility of, interstate commerce;

be fined not more than two times the amount of the gain directly or indirectly derived from the offense or $50,000, whichever is higher, or imprisoned not more than five years, or both.

"(b) Whoever intentionally and without authorization damages a computer described in subsection (a) shall be fined not more than $50,000 or imprisoned not more than five years or both.

"(c) DEFINITIONS.—For the purpose of this section, the term—

"(1) 'computer' means a device that performs logical, arithmetic, and storage functions by electronic manipulation, and includes any property and communi-

BEST COPY AVAILABLE

cation facility directly related to or operating in conjunction with such a device; but does not include an automated typewriter or typesetter, or any computer designed and manufactured for, and which is used exclusively for routine personal, family, or household purposes including a portable hand-held electronic calculator;

"(2) 'financial institution' means—

"(A) a bank with deposits insured by the Federal Deposit Corporation;

"(B) a member of the Federal Reserve including any Federal Reserve bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal home loan bank systems and any home loan bank;

"(F) a member or business insured by the Securities Investor Protection Corporation; and

"(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities and Exchange Act of 1934;

"(3) 'property' means anything of value, and includes tangible and intangible personal property, information in the form of electronically processed, produced, or stored data, or any electronic data processing representation thereof, and services;

"(4) 'services' includes computer data processing and storage functions;

"(5) 'United States Government' includes a branch or agency thereof; and

"(6) 'use' includes to instruct, communicate with, store data in, or retrieve data from, or otherwise utilize the logical, arithmetic, or memory functions of a computer.

"(d)(1) In a case in which Federal jurisdiction over an offense as described in this section exists concurrently with State or local jurisdiction, the existence of Federal jurisdiction does not, in itself, require the exercise of Federal jurisdiction, nor does the initial exercise of Federal jurisdiction preclude its discontinuation.

"(2) In a case in which Federal jurisdiction over an offense as described in this section exists or may exist concurrently with State or local jurisdiction, Federal law enforcement officers, in determining whether to exercise jurisdiction, should consider—

"(A) the relative gravity of the Federal offense and the State or local offense;

"(B) the relative interest in Federal investigation or prosecution;

"(C) the resources available to the Federal authorities and the State or local authorities;

"(D) the traditional role of the Federal authorities and the State or local authorities with respect to the offense;

"(E) the interests of federalism; and

"(F) any other relevant factor.

"(3) The Attorney General shall—

"(A) consult periodically with representatives of State and local governments concerning the exercise of jurisdiction in case in which Federal jurisdiction as described in this section exists or may exist concurrently with State or local jurisdiction;

"(B) provide general direction to Federal law enforcement officers concerning the appropriate exercise of such Federal jurisdiction;

"(C) report annually to Congress concerning the extent of the exercise of such Federal jurisdiction during the preceding fiscal year; and

"(D) report to Congress, within one year of the effective date of this Act, on the long-term impact

BEST COPY AVAILABLE

upon Federal jurisdiction, of this Act and, the increasingly pervasive and widespread use of computers in the United States. The Attorney General shall periodically review and update such report.

"(4) Except as otherwise prohibited by law, information or material obtained pursuant to the exercise of Federal jurisdiction may be made available to State or local law enforcement officers having concurrent jurisdiction, and to State or local authorities otherwise assigned responsibility with regard to the conduct constituting the offense.

"(5) An issue relating to the propriety of the exercise of, or of the failure to exercise, Federal jurisdiction over an offense as described in this section, or otherwise relating to the compliance, or to the failure to comply, with this section, may not be litigated, and a court may not entertain or resolve such an issue except as may be necessary in the course of granting leave to file a dismissal of an indictment, an information, or a complaint.".

SEC. 4. The table of sections of chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following:

"1028. Computer fraud and abuse.".

O

BEST COPY AVAILABLE